Identity Theft and Account Takeovers becoming common in Fresno

Account takeover occurs when a criminal obtains your existing credit card or bank account information, and then attaches themselves to those accounts. The criminal gets name, social security number, and with a little internet research, they can learn enough about you to **run your credit report for you**. Once they have this, they know your bank and credit account numbers. All they have to do then is go shopping with your credit cards. You will find out about this when you get your bill. You don't have credit cards where they want to shop! They get new credit cards for you. By the time these cards are sent to your home, the suspects have already used them, either through internet purchases or providing your social security number at the store. Some businesses are so effective, that they allow the new credit recipient to obtain shopping passes for use while waiting for the credit card to arrive.

How does the criminal get your social security number? The most common method is simple theft. This can be stealing a purse or wallet from a person, vehicle, or home. The theft can also occur from businesses you legitimately gave your social security number to; such as a doctor, dentist, Real Estate Company, a place you got a loan, etc.

Credit reports are available to consumers free at www.annualcreditreport.com. The person running the report needs to know their social security number and basic facts about themselves. The questions are multiple choice, and if you answer the questions correctly, you are emailed a credit report. When the criminal runs the report, they can frequently guess the correct answers. Why? The answers are often readily available on the internet or through social networking sites.

The credit card part of the fraud can be bothersome; it can negatively affect your credit rating, and cause you to spend hours contacting creditors, gathering information and the recovery process can last months and years. But even more devastating is when they attack your checking or savings account. Some criminals have the ability to set up your account for internet banking, and then they have full access to your accounts. A few tech savvy criminals have hacked into existing internet accounts, changed your password and locked you out of your own accounts. Fortunately, this is rare.

Preventing Financial Fraud and Identity theft is more important than ever. Criminals are using more innovative ways to gain access to financial information; thereby making everyone more vulnerable to attack. Preventing Identity theft takes a little effort, but the effort is minute compared to the time and effort required to fix the problems associated with the crime. Prevention Techniques:

- Protect your social security number. Your social security number is the key. The suspects cannot run your credit report until they obtain your social security number.
    - Memorize your social security number.
    - Do not carry your social security number with you. If your purse or wallet is stolen, the thief has a window into your life.

    - Don't leave your card at home where a criminal can find it. Put your social security card in a safe deposit box. Documents that display your social security number, such as tax returns, should be secured in a locked file or safe deposit box.
    - Never give out the number except when absolutely necessary.
        - Even if it is on a form you are filling out, it might not be required. Your number is only as safe as those you have given it to; protect your social.
    - When you have to give your social security number, ask about how the business protects that information. Let them know you are concerned about Identity theft.
- Shred documents with personal or financial information
- Run your credit report. If you run your reports annually, the criminal cannot run it for you.
- Establish an online relationship with your financial institutions. This includes credit card companies as well as your bank or credit union. Most have an alert system which can notify you of any changes to your account within minutes or days of any usage or changes to your account. It's a great tool to catch fraudulent activity quickly.
    - Use a strong password. This is usually a combination of letters and numbers with special characters.
        - Never use your mother's maiden name
        - Never use the name of your child
        - Never use your address

If you become a victim, be sure you make a Police Report regarding the ID theft. Notify your Financial Institutions immediately. If you discover a criminal has run your credit report for you, be sure to notify every credit card company or bank that you have a relationship with. Put a fraud alert on your social security with the credit bureaus.

- Fresno City residents can make a report online at www.fresno.gov/reportcrime
- When you notify the credit card companies and banks, you may learn critical information that can help the police identify the suspect. This information needs to be shared with law enforcement. Fresno victims can email information and documents to financialcrimes@fresno.gov or fax to 621-6332.